

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
GREENEVILLE DIVISION

FILED

SEP 29 2017

Clerk, U. S. District Court
Eastern District of Tennessee
At Greeneville

IN RE THE SEARCH OF:

- (1) HP LAPTOP COMPUTER BEARING
SERIAL NUMBER CND7124NT2;
- (2) CRUZER GLIDE 32GB THUMB
DRIVE;
- (3) CRUZER GLIDE 16GB THUMB
DRIVE;
- (4) APPLE IPHONE A1687, FCC ID:
BCG-E2944A; AND
- (5) APPLE IPHONE A1661, DCC ID:
BCG-E3087A

CURRENTLY IN THE POSSESSION OF
THE UNITED STATES SECRET
SERVICE IN GREENEVILLE,
TENNESSEE

MISC. NO. 2:17-mj-200

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Thomas Whitehead, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AFFIANT BACKGROUND

(1) I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of the electronic devices listed in the caption to this affidavit (the "captioned items") and further described in Attachment A, which are currently in the possession of the United States Secret Service in Greeneville, Tennessee, and the extraction from that property of the electronically stored information described in Attachment B.

(2) This Affidavit sets forth facts establishing probable cause to believe that Amaurys Mendez Campanon and Odemnis Prats Leiva, and one or more other as-of-yet unidentified

people, have committed violations of 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1028A (Aggravated Identity Theft), and 18 U.S.C. §§ 1956 and 1957 (Money Laundering) (collectively, the “specified crimes”), and that evidence of the specified crimes, including the items set forth on Attachment B, are located on the captioned items.

Affiant Background

(3) I am a Special Agent with the U.S. Secret Service, currently assigned to the Greeneville Domicile Office, Greeneville, TN. I have been employed as a federal law enforcement agent since February 2003. As a Special Agent, I have been involved with numerous criminal investigations to include counterfeit currency, credit card fraud, bank fraud, access device fraud, identity theft, wire fraud, money laundering and various other crimes. I have executed many arrests, search and seizure warrants in my years as a Special Agent. The following facts are known to me and or to officers of the Kingsport Police Department. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. The facts in this affidavit come from information obtained in the course of an ongoing investigation.

PROBABLE CAUSE

(4) The facts in this Affidavit are derived from my personal observations, my training and experience, and information obtained from various witnesses, video surveillance footage, and documents obtained during the investigation. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this investigation.

(5) In September 2017, a federal grand jury sitting in Greeneville, Tennessee returned an indictment charging Amaurys Mendez Campanon and Odemnis Prats Leiva with conspiracy

(18 U.S.C. § 371), wire fraud (18 U.S.C. § 1343), and aggravated identity theft (18 U.S.C. § 1028A) based in part upon some of the evidence described in this affidavit. At the time that the case was presented to the grand jury, I suspected – as further described in this affidavit and based upon my training and experience – that the captioned items contained evidence of additional examples of the specified crimes, and would identify other as-of-yet unidentified persons committing the specified crimes.

(6) In summary, this Affidavit is intended to show that the items described on Attachment B are stored on the captioned items, are *themselves* evidence of the specified crimes, contain further evidence of the specified crimes, will identify additional victims of the specified crimes, and will identify other participants in the specified crimes.

(7) On 08/10/17, I was contacted by Detective Martin Taylor of the Kingsport Police Department (“KPD”) regarding two individuals – AMAURYS MENDEZ COMPANON and PRATS LEVIA ODEMNIS – that the Rogersville Police Department (“RPD”) had in custody for the commission of credit card fraud. Det. Taylor stated that the RPD was requesting assistance with this investigation. I then contacted Det. Travis Fields of the RPD. Det. Fields stated that AMAURYS MENDEZ COMPANON AND PRATS LEVIA ODEMNIS had committed credit card fraud and were believed to have re-encoded credit/debit cards in their possession. A re-encoded credit/debit card is an access device that contains a stolen account number that has been placed onto the magnetic stripe of a plastic card, together with other information such as the account owner’s full name.

(8) Later that same day I responded to the RPD and met with Det. Fields. Det. Fields stated that he had received a call from Lisa Crawford of Eastman Credit Union at approximately 1630 hours. Ms. Crawford told Det. Fields that 2 unknown individuals had fraudulently used

Eastman Credit Union debit/credit cards in the past couple of days and compiled upwards of \$20,000 in fraud. Ms. Crawford told Det. Fields that fraudulent purchases had been made at the Walmart located at 4331 Highway 66 S, Rogersville, TN 37857, less than an hour ago.

(9) On August 10, 2017, Det. Fields then contacted Walmart loss prevention officer Mike Campbell and provided him the information received from Ms. Crawford. Mr. Campbell was able to locate the individual – who turned out to be Leiva – and provided Det. Fields with surveillance photographs of an individual wearing a sling on his right arm. Mr. Campbell then stated that the suspect (Leiva) was still inside the Walmart in Rogersville, TN at that moment. Det. Fields and other RPD officers responded to that Walmart. Mr. Campbell notified Det. Fields that, moments earlier, the suspect exited the Walmart and entered into a Gray Nissan Pathfinder. Det. Fields and RPD Officers were able to stop the vehicle before it exited the parking area. Det. Fields placed the passenger (Leiva) and the driver (Campanon) under arrest.

(10) At the time of their arrest, Campanon was in possession of seven unlawfully re-encoded access devices and two gift cards, and Leiva was in possession of nine unlawfully re-encoded access devices, \$7,020.25 in cash, numerous gift cards, and a Cruzor Glide 16GB Thumb Drive, which is one of the captioned items describe on Attachment A.

(11) After arresting Leiva and Campanon, police obtained a State-issued search warrant to search the rented Nissan Pathfinder that Campanon was driving prior to his arrest. Inside the vehicle, law enforcement found the following:

(a) a black backpack containing the HP laptop bearing serial number CND7124NT2, which is one of the captioned items described on Attachment A;

(b) the Cruzor Glide 32GB thumb drive, which is one of the captioned items described on Attachment A;

(c) an Apple iPhone A1687, FCC ID: BCG-E2944A, which is one of the captioned items described on Attachment A;

(d) an Apple iPhone A1661, DCC ID: BCG-E3087A, which is one of the captioned items described on Attachment A; and

(e) miscellaneous other items that are evidence of the specified crimes, including (i) an MSRX6 card encoder; (ii) either counterfeit credit / debit cards; (iii) \$4,400 in cash; (iv) a brown suitcase containing six gift cards unlawfully re-encoded with stolen account numbers one counterfeit credit/debit card, eight Vanilla gift cards, two Visa debit gift cards, and 1 Subway gift card; (v) a gray shoe inside the brown suitcase containing five Vanilla gift cards, one Visa debit gift card, and \$4,460 in cash; (vi) eight counterfeit credit/debit cards bearing the name "Odemnis Prats Leiva" were located in the center console of the vehicle; (vii) seven counterfeit credit/debit cards bearing the name "Amaurys Mendez" were located in the vehicle's glove box; and (viii) approximately 26 MoneyGram and Western Union money orders for various amounts ranging from \$100 to \$900 and totaling \$16,700.

(12) Based upon my training and experience, I know that people who engage in credit-card schemes like these:

(a) use card encoders (like the MSRX6 card encoder found in the suspects' vehicle) together with a computer (like the captioned HP computer found in the suspects' vehicle) to re-encode cards with stolen account information (like the cards re-encoded with stolen account information found in the suspects' vehicle);

(b) use thumb drives like the captioned Cruiser Glide 32GB and 16GB thumb drives found in the suspect's vehicle and on Leiva's person to store evidence of the specified crimes; and

(c) use smart phones like the two captioned Apple iPhones found in the suspects' vehicle to send communications, take pictures, and use the GPS capabilities in furtherance of, and other facilitate, the specified crimes.

(13) I know that Campanon and Leiva swiped several of the access devices that had been unlawfully re-encoded with account information for the following reasons:

(a) I reviewed the surveillance footage for the Greeneville, TN Walmart provided by the GPD. That footage depicts Leiva swiping a card at an ATM inside the Walmart located in Greeneville, TN on August 7, 2017. I have received and reviewed transaction receipts from Eastman Credit Union. These transaction receipts show that account number **** * 3778 belonging to R.M. was swiped at that Walmart at 14:34 hours on August 7, 2017, without the authority of the account owner, R.M.

(b) I reviewed the surveillance footage for the Greeneville, TN Walmart that was provided by the GPD. That footage depicts Leiva swiping a card at an ATM inside the Walmart located in Greeneville, TN on August 7, 2017. I have received and reviewed transaction receipts from Eastman Credit Union. These transaction receipts show account number **** * 7514 belonging to H.B. was swiped at Walmart at 14:16 hours and 14:17 hours on August 7, 2017, without the authority of the account owner, H.B.

(c) I reviewed the surveillance footage from the Walmart located in Johnson City, TN that was provided by the JCPD. The footage depicts Leiva inside the Walmart in Johnson City, TN using an ATM at approximately 19:22 hours on August 7, 2017. A transaction report provided by the Bank of Tennessee for account number **** * 9241 belonging to R.D.M. shows a fraudulent ATM withdrawal occurring at 19:22 hours on August 7, 2017, at the Walmart located in Johnson City, TN.

(d) I reviewed the surveillance footage and transaction reports for the Walmart located in Johnson City, TN that was provided by the JCPD. The footage and transaction reports depict Campanon attempting to purchase a money order by swiping account number **** * 3589 which belongs to K.W. at approximately 19:25 hours on August 7, 2017.

(e) I reviewed the surveillance footage for the Walmart located in Bristol, TN that was provided by the BPD. That footage depicts Leiva inside the Walmart in Bristol, TN on August 9, 2017, purchasing a money order, making ATM withdrawals, and making a purchase of Ensure liquid. Transaction records provided by Walmart show the account number belonging to J.B. (**** * 0749) being used at approximately 14:12 hours to purchase the Ensure liquid and 14:16 hours to purchase a money order. Surveillance photos show Leiva using an ATM machine located inside Walmart at 14:19 hours. Leiva is then seen leaving the area in a gray SUV similar to the one he was arrested in by the RPD.

(f) I reviewed the surveillance footage from the Walmart located in Bristol, VA that was provided to me by the Washington County, VA Sheriff's Department. That footage depicts Leiva inside the Walmart in Bristol, VA on August 9, 2017, using an ATM machine from approximately 18:12 hours until 18:19 hours. A transaction report provided by Eastman Credit Union shows that 2 fraudulent ATM withdrawals were made at 18:13 hours and 18:14 hours using account number **** * 2888 which belongs to T.M. LLC.

(g) On August 10, 2017, Campanon was found in possession of a card that was encoded with a stolen account number (**** * 0252) that belongs to T.F. That account was used fraudulently without the authority of the account holder, T.F., at the Walmart in Rogersville, TN, for one transaction at 15:29 hours.

(h) On August 10, 2017, Leiva was found in possession of a card that was encoded with a stolen account number (**** * 2147) that belongs to B.S. That account was used fraudulently without the authority of the account holder, B.S., at the Walmart in Rogersville, TN, for two separate transactions at 15:36 hours and 15:54 hours respectively. Walmart Loss Prevention Officer Mike Campbell confirmed to Det. Fields that Leiva was inside the Walmart in Rogersville, TN making purchases during this time period.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

(14) Based on my knowledge, training, and experience, I know that electronic devices like the captioned items can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

(15) *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the items were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the captioned items because:

(a) Data on storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

(b) Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

(c) A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

(d) The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

(e) Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

(16) *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the captioned devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

(17) *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

(18) Based on the information contained in this Affidavit, as well as Affiant's training and experience, your Affiant believes there is probable cause to believe that Amaurys Mendez Campanon and Odemnis Prats Leiva, and one or more other as-of-yet unidentified people, have committed violations of the specified crimes, and that there is probable cause to believe that the captioned items have been used in furtherance of the specified crimes and contain evidence of the specified crimes.

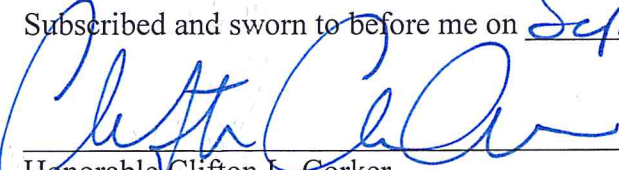
* * * * *

Respectfully submitted,



Thomas Whitehead, Special Agent
United States Secret Service

Subscribed and sworn to before me on September 29, 2017



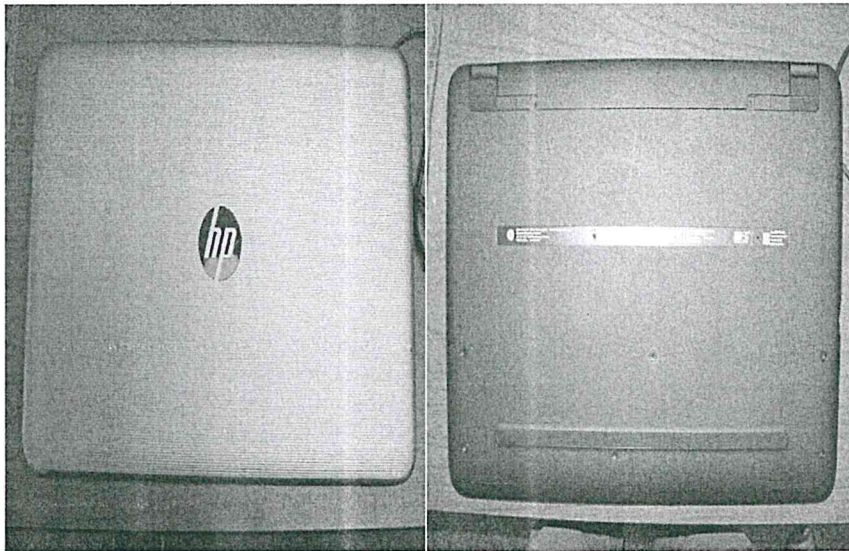
Honorable Clifton L. Corker
United States Magistrate Judge

Attachment A

**PROPERTY TO BE SEARCHED
Search Warrant Affidavit**

The property to be searched is:

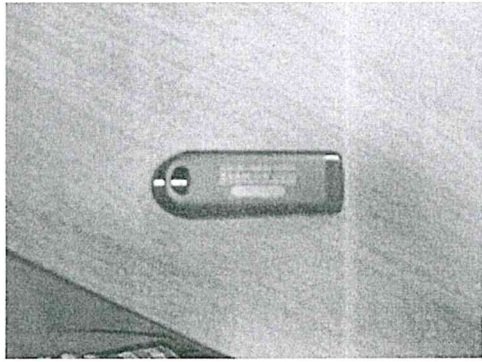
- (1) HP laptop computer bearing serial number CND7124NT2



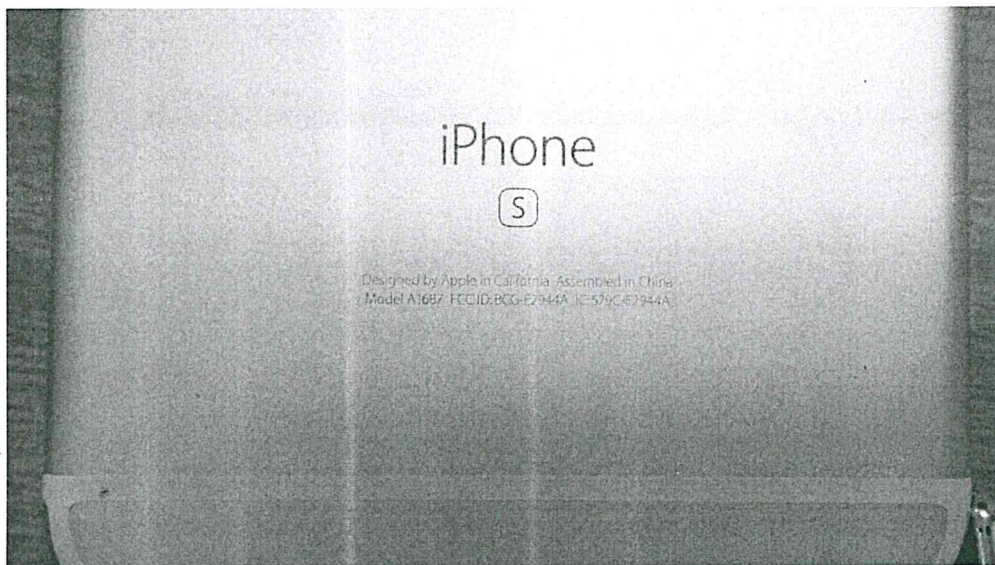
- (2) Cruzer Glide 32GB thumb drive



- (3) Cruzer Glide 16GB thumb drive



(4) Apple iPhone A1687, FCC ID: BCG-E2944A



(5) Apple iPhone A1661, DCC ID: BCG-E3087A



Attachment B

ITEMS TO BE SEIZED

Search Warrant Affidavit

All information, whether stored in physical or electronic format, described in the Affidavit that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1028A (Aggravated Identity Theft), and 18 U.S.C. §§ 1956 and 1957 (Money Laundering) (collectively, the “specified crimes”):

(1) All records on any of the items described on Attachment A that relate to violations of the specified crimes and involve one or more of Amaurys Mendez Campanon, Odemnis Prats Leiva, or other unidentified co-conspirators, including:

- (a) Contact lists;
- (b) Call logs;
- (c) Text or Multimedia messages;
- (d) Internet browser history;
- (e) Web pages;
- (f) Search terms;
- (g) Cell tower/GPS history;
- (h) Wireless network connection history;
- (i) Chat messages;
- (j) Emails or other electronic communications;
- (k) Photographs;
- (l) Deleted files;
- (m) File transfer logs;
- (n) Stolen account numbers;
- (o) Card encoding software applications;
- (p) Other documents, records, files, or information evidencing the commission of the specified crimes.

(2) Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;